CRYPTOGRAPHIC SYSTEM WITH METHODS FOR USER-CONTROLLED MESSAGE RECOVERY

Abstract of the Disclosure

A cryptosystem is described which automatically provides an extra "message recovery" recipient(s) when an encrypted message is generated in the system. The system is typically configured such that the extra recipient or "message recovery agent" (MRA) -- an entity which itself has a public key (i.e., a MRA public key) -- is automatically added, under appropriate circumstances, as a valid recipient for an encrypted message created by a user. In a corporate setting, for example, the message recovery agent is the "corporate" message recovery agent designated for that company (firm, organization, or other group) and the user is an employee (or member) of that company (or group). In operation, the system embeds a pointer (or other reference mechanism) to the MRA public key into the public key of the user or employee, so that encrypted messages sent to the company's employees from outside users (e.g., those individuals who are not employees of the company) can nevertheless still be recovered by the company. Alternatively, the MRA public key itself can be embedded within the public key of the employee or user (i.e., a key within a key), but typically at the cost of increasing the storage requirement of the user's key. By including in the user's key (e.g., an employee) a pointer to a message recovery agent's key (or the MRA key itself), the system provides a mechanism for assisting a user outside a group (e.g., a user who is outside a particular company) with the task of including in an automatic and non-intrusive manner the key of an additional recipient, such as one intended for message recovery.